

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 8 - 3 3 5 0 4 0

(43) 公開日 平成 8 年 (1996) 12 月 17 日

(51) Int. Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G09C 1/00		7259-5J	G09C 1/00	
H04H 1/00			H04H 1/00	F
1/02			1/02	E
H04L 9/00			H04L 9/00	Z
9/10			H04N 7/167	

審査請求 未請求 請求項の数 5 F D (全 12 頁) 最終頁に続く

(21) 出願番号 特願平 7 - 1 5 9 7 7 1

(22) 出願日 平成 7 年 (1995) 6 月 2 日

(71) 出願人 0 0 0 0 5 2 2 3

富士通株式会社

神奈川県川崎市中原区上小田中 4 丁目 1 番  
1 号

(72) 発明者 秋山 良太

神奈川県川崎市中原区上小田中 1 0 1 5 番  
地 富士通株式会社内

(72) 発明者 宗像 昭夫

神奈川県川崎市中原区上小田中 1 0 1 5 番  
地 富士通株式会社内

(74) 代理人 弁理士 遠山 勉 (外 1 名)

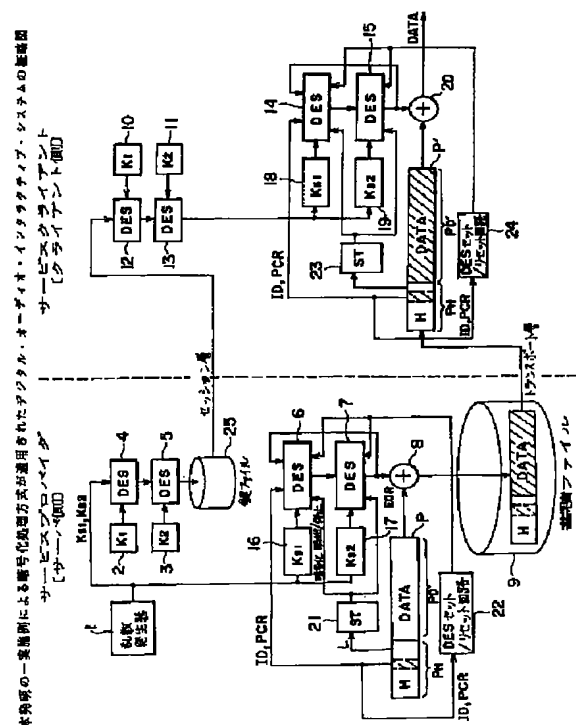
最終頁に続く

(54) 【発明の名称】 暗号化処理方式

(57) 【要約】

【目的】 暗号化アルゴリズムを強化することによって鍵の頻繁な変更を減らし、サービスプロバイダーサービスクライアント間の情報転送効率を向上させることができる暗号化処理方式を提供する。

【構成】 乱数発生器 1 は、乱数に基づき第 1 タイトル鍵  $Ks1$  及び第 2 タイトル鍵  $Ks2$  を生成する。タイトル用第 1 DES 暗号化回路 6 は、入力情報を第 1 タイトル鍵  $Ks1$  によって暗号化する。この入力情報の初期値は、パケットのヘッダから抽出されたデータ識別 ID 及び相対時刻情報 (PCR) である。初期値の暗号化を完了した後では、タイトル用第 2 DES 暗号化回路 7 の暗号化結果が入力情報となる。このタイトル用第 2 DES 暗号化回路 7 は、タイトル用第 1 DES 暗号化回路 6 による暗号化結果値を第 2 タイトル鍵  $Ks2$  によって暗号化する。排他 OR 回路 8 は、パケットに格納されたデータとタイトル用第 2 DES 暗号化回路 7 の暗号化結果値との排他論理和を出力する。これが暗号化データとなる。



## 【特許請求の範囲】

【請求項 1】データを提供するサービスプロバイダとデータの供給を受けるサービスクライアントとの間で配送される前記データを暗号化する暗号化処理方式において、

前記サービスプロバイダは、

乱数に基づき 2 つの鍵を生成する鍵生成手段と、

この鍵生成手段により生成された 2 つの鍵によりデータを暗号化する第 1 の暗号化手段と、

この第 1 の暗号化手段によって暗号化された前記データを前記サービスクライアントに配送するデータ配送手段と、

前記 2 つの鍵を特定内容のマスタ鍵によって暗号化する第 2 の暗号化手段と、

この第 2 の暗号化手段によって暗号化された前記 2 つの鍵を前記サービスクライアントに配送する鍵配送手段とを備え、

前記サービスクライアントは、

前記鍵配送手段によって配送された前記暗号化された 2 つの鍵を前記特定内容のマスタ鍵によって復号化する第 1 の復号化手段と、

この第 1 の復号化手段によって復号化された前記 2 つの鍵により前記データ配送手段によって配送された前記暗号化されたデータを復号化する第 2 の復号化手段とを備えたことを特徴とする暗号化処理装置。

【請求項 2】パケットに格納されたデータをサービスクライアントに配送するサービスプロバイダにおける暗号化処理方式において、

乱数に基づき第 1 の鍵及び第 2 の鍵を生成する鍵生成手段と、

入力情報を前記第 1 の鍵によって暗号化する第 1 の暗号化回路と、

前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第 1 の暗号化回路に前記入力情報の初期値として入力する抽出手段と、

前記第 1 の暗号化回路による暗号化結果値を前記第 2 の鍵によって暗号化するとともに、この暗号化結果値を前記第 1 の暗号化回路に前記入力情報として更新入力する第 2 の暗号化回路と、

前記パケットに格納されたデータと前記第 2 の暗号化回路の暗号化結果値との排他論理和を出力する排他 OR 回路とを備えたことを特徴とする暗号化処理方式。

【請求項 3】前記パケットは、このパケットに格納されているデータの格納位置についての格納位置情報を含んでいるとともに、

この格納位置情報に基づいて、前記データが前記排他 OR 回路に入力されている時点でのみ前記第 1 の暗号化回路及び前記第 2 の暗号化回路による暗号化を可能とする暗号化制御回路とを更に備えたことを特徴とする請求項 2 記載の暗号化処理装置。

【請求項 4】前記パケットから前記時刻情報を検出して、前記第 1 の暗号化回路及び前記第 2 の暗号化回路の状態を初期化する初期化手段を更に備えたことを特徴とする請求項 2 記載の暗号化処理装置。

【請求項 5】データを提供するサービスプロバイダとデータの供給を受けるサービスクライアントとの間でパケットに格納されて配送される前記データを暗号化する暗号化処理方式において、

前記サービスプロバイダは、

乱数に基づき第 1 の鍵及び第 2 の鍵を生成する鍵生成手段と、

この第 1 の鍵及び第 2 の鍵を前記サービスクライアントに配送する鍵配送手段と、

入力情報を前記第 1 の鍵によって暗号化する第 1 の暗号化回路と、

前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第 1 の暗号化回路に前記入力情報の初期値として入力する第 1 の抽出手段と、

前記第 1 の暗号化回路による暗号化結果値を前記第 2 の鍵によって暗号化するとともに、この暗号化結果値を前記第 1 の暗号化回路に前記入力情報として更新入力する第 2 の暗号化回路と、

前記パケットに格納されたデータと前記第 2 の暗号化回路の暗号化結果値との排他論理和を出力する第 1 の排他 OR 回路と、

この排他 OR 回路から出力されデータを格納した前記パケットを前記サービスクライアントに配送するデータ配送手段とを備え、

前記サービスクライアントは、

入力情報を前記第 1 の前記鍵配送手段によって配送された前記第 3 の鍵によって暗号化する第 3 の暗号化回路と、

前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第 1 の暗号化回路に前記入力情報の初期値として入力する第 2 の抽出手段と、

前記第 3 の暗号化回路による暗号化結果値を前記第 2 の鍵によって暗号化するとともに、この暗号化結果値を前記第 3 の暗号化回路に前記入力情報として更新入力する第 4 の暗号化回路と、

前記パケットに格納されたデータと前記第 4 の暗号化回路の暗号化結果値との排他論理和を出力する第 2 の排他 OR 回路とを備えたことを特徴とする暗号化処理方式。

【発明の詳細な説明】

【0 0 0 1】

【産業上の利用分野】本発明は、クライアントからの要求に応じて、映像著作物等のソフトウェアを通信手段を介して配送するシステム（デジタル・オーディオ・インタラクティブ・システム）において、特定の鍵によってこのソフトウェアを暗号化するための暗号化処理方式に関する。

## 【 0 0 0 2 】

【従来の技術】近年、ケーブルテレビジョンシステムや通信衛星を用いた通信システムの構築を背景に、デジタル情報化されたソフトウェア（音声データ、映像データ等、以下、「データ」という）を各家庭等に配送するサービスが提案されている。このサービスシステムは、ビデオ・オン・デマンド方式等と呼ばれるデジタル・オーディオ・インタラクティブ・システムである。このデジタル・オーディオ・インタラクティブ・システムにおいては、サービス提供者とユーザとの間で電話線等を介した通信が行われる。そして、サービス提供者は、ユーザから要求された時刻に要求された内容のデータをこのユーザに配送するとともに、このデータの使用料金をクレジットカード会社等を通じて当該ユーザに課金し、その一部をコンテンツ供給者に還元するのである。

【 0 0 0 3 】このようなデジタル・オーディオ・インタラクティブ・システムが普及してゆく上で重要な事は、インフラストラクチャーとなるサーバ/ネットワーク/ターミナルが低コストで構築されることは勿論であるが、これらを媒介としてユーザに提供されるデータが豊富に準備されなければ、成功とはならないということである。即ち、データとインフラストラクチャーは車の両輪であるので、データ提供者がコンテンツ提供による利益回収を見込めるとともに不測の損害を被る危険がない仕組みをこのインフラストラクチャーに組み込むことにより、データが集まりやすい環境を整備することが不可欠なのである。なお、このような仕組みは、データ提供者とユーザとを媒介する供給メディアの種類（広帯域ケーブルネットワーク、衛星システム、移動通信、光メディアパッケージ等）に拘わらず、整備されていなければならない。

【 0 0 0 4 】従って、配送中においてデータが無権利の第三者（当該データの使用料を支払っていない第三者）に傍受されて不当に使用（再生）されることがないように、配送中においてデータは暗号化されていた。従来における暗号化処理方式を、図 6 によって説明する。

【 0 0 0 5 】図 6 において、サービスプロバイダ（サービス提供者側システムのことをいう。以下同じ）の第 1 暗号化回路 1 0 3 は、パケットフォーマットのデータを一個の鍵（K s）のみで暗号化し、トランスポート層伝送路を通じてサービスクライアント（ユーザ側システムのことをいう。以下同じ）に配送する。この暗号化されたデータを受け取ったサービスクライアントの第 1 復号化回路 1 0 6 は、第 1 暗号化回路 1 0 3 にて暗号化に用いられた鍵（K s）により、データを復号化する。このように従来の暗号化処理方式ではデータの暗号化及び復号化のアルゴリズムは一個の鍵（K s）を用いた一段階のみの脆弱なものであったので、鍵（K s）の解読を防ぐため、鍵（K s）を頻繁に変更する必要があった。また、通信路の誤り及び切断から速やかに復旧する為、暗

号同期信号を送信することが必要であった。

【 0 0 0 6 】この条件を満足するため、図 6 に示すように、サービスプロバイダに乱数発生器 1 0 0、マスタ鍵（K 1）1 0 1 及び第 2 暗号化回路 1 0 2 を設け、サービスクライアントに、マスタ鍵（K 1）1 0 4 及び第 2 復号化回路 1 0 2 を設けている。

【 0 0 0 7 】この乱数発生器 1 0 0 は、常時継続的に乱数系列を発生している。そして、この乱数系列が数秒間隔で鍵ブロック単位（予め定められた鍵の桁）で切り出され、数秒間隔で更新される鍵（K s）として第 1 暗号化回路 1 0 3 に入力される。このように更新される鍵（K s）はサービスクライアントにも配送されなければならないので、第 2 の暗号化回路 1 0 2 は、乱数発生器 1 0 0 から切り出される鍵（K s）をマスタ鍵（K 1）1 0 1 で暗号化し、トランスポート層のユーザ割当パケットの一部（セッション層）を利用してサービスクライアントに配送する。サービスクライアントの第 2 復号化回路 1 0 5 は、暗号化された鍵（K s）をマスタ鍵（K 1）を用いて復号化し、第 1 復号化回路 1 0 6 に入力していた。

【 0 0 0 8 】そして、第 1 暗号化回路 1 0 3 及び第 1 復号化回路 1 0 6 は、新たな鍵（K s）の入力がある毎に自らをリセットして同期を取り、それ以降のデータを新たな鍵（K s）によって暗号化・復号化する。なお、マスタ鍵（K 1）1 0 1、1 0 4 は、サービスプロバイダ及びサービスクライアントに、夫々予め同内容で用意された固定鍵である。

【 0 0 0 9 】このようにして、従来のデータ暗号化処理方式では、鍵（K s）の変更及び暗号同期処理を行っていた。

## 【 0 0 1 0 】

【発明が解決しようとする課題】しかしながら、上記従来の暗号化処理方式にあっては、数秒間隔で、新たな鍵（K s）をサービスプロバイダからサービスクライアントに配送しなければならないので、本来のデータ配送に使用するパケット以外に、大量のパケット（鍵配送用パケット）を転送しなければならなかった。その結果、サービスプロバイダーサービスクライアント間の情報転送効率が著しく低下してしまっていた。

【 0 0 1 1 】本発明の第 1 の課題は、暗号化アルゴリズムを強化することによって鍵の頻繁な変更の必要を減らし、サービスプロバイダーサービスクライアント間の情報転送効率を向上させることができる暗号化処理方式を提供することである。

【 0 0 1 2 】また、本発明の第 2 の課題は、データの転送に用いるパケットヘッダ上の相対時刻情報を暗号化の初期値に利用して、同じ内容のデータを発生時刻に依り別内容の暗号化データとし、解読を困難にすることができる暗号化処理方式を提供することである。

## 【 0 0 1 3 】

## 【課題を解決するための手段】

(第1の態様) 本発明の第1の態様は、専ら上記第1の課題を、サービスプロバイダーサービスクライアント間で解決するためになされたものである。即ち、図1の原理図に示したように、データを提供するサービスプロバイダとデータの供給を受けるサービスクライアントとの間で配送される前記データを暗号化する暗号化処理方式において、前記サービスプロバイダは、乱数に基づき2つの鍵(Ks1, Ks2)を生成する鍵生成手段(乱数発生器110)と、この鍵生成手段(乱数発生器110)により生成された2つの鍵(Ks1, Ks2)によりデータを暗号化する第1の暗号化手段(113)と、この第1の暗号化手段(113)によって暗号化された前記データを前記サービスクライアントに配送するデータ配送手段(トランスポート層伝送路)と、前記2つの鍵(Ks1, Ks2)を特定内容のマスタ鍵(K1, 101)によって暗号化する第2の暗号化手段(112)と、この第2の暗号化手段(112)によって暗号化された前記2つの鍵(Ks1, Ks2)を前記サービスクライアントに配送する鍵配送手段(セッション層伝送路)とを備え、前記サービスクライアントは、前記鍵配送手段(セッション層伝送路)によって配送された前記暗号化された2つの鍵(Ks1, Ks2)を前記特定内容のマスタ鍵(K1, 114)によって復号化する第1の復号化手段(115)と、この第1の復号化手段(115)によって復号化された前記2つの鍵(Ks1, Ks2)により前記データ配送手段(トランスポート層伝送路)によって配送された前記暗号化されたデータを復号化する第2の復号化手段(116)とを備えたことを特徴とする(請求項1に対応)。

(第2の態様) 本発明の第2の態様は、上記第1及び第2の課題を、サービスプロバイダ側で解決するためになされたものである。即ち、パケットに格納されたデータをサービスクライアントに配送するサービスプロバイダにおける暗号化処理方式において、乱数に基づき第1の鍵及び第2の鍵を生成する鍵生成手段と、入力情報を前記第1の鍵によって暗号化する第1の暗号化回路と、前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第1の暗号化回路に前記入力情報の初期値として入力する抽出手段と、前記第1の暗号化回路による暗号化結果値を前記第2の鍵によって暗号化するとともに、この暗号化結果値を前記第1の暗号化回路に前記入力情報として更新入力する第2の暗号化回路と、前記パケットに格納されたデータと前記第2の暗号化回路の暗号化結果値との排他論理和を出力する排他OR回路とを備えたことを特徴とする(請求項2に対応)。

(第3の態様) 本発明の第3の態様は、上記第1及び第2の課題を、サービスプロバイダーサービスクライアント間で解決するためになされたものである。即ち、データを提供するサービスプロバイダとデータの供給を受け

るサービスクライアントとの間でパケットに格納されて配送される前記データを暗号化する暗号化処理方式において、前記サービスプロバイダは、乱数に基づき第1の鍵及び第2の鍵を生成する鍵生成手段と、この第1の鍵及び第2の鍵を前記サービスクライアントに配送する鍵配送手段と、入力情報を前記第1の鍵によって暗号化する第1の暗号化回路と、前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第1の暗号化回路に前記入力情報の初期値として入力する第1の抽出手段と、前記第1の暗号化回路による暗号化結果値を前記第2の鍵によって暗号化するとともに、この暗号化結果値を前記第1の暗号化回路に前記入力情報として更新入力する第2の暗号化回路と、前記パケットに格納されたデータと前記第2の暗号化回路の暗号化結果値との排他論理和を出力する第1の排他OR回路と、この排他OR回路から出力されデータを格納した前記パケットを前記サービスクライアントに配送するデータ配送手段とを備え、前記サービスクライアントは、入力情報を前記第1の前記鍵配送手段によって配送された前記第1の鍵によって暗号化する第3の暗号化回路と、前記パケットのヘッダから時刻情報を抽出し、この時刻情報を前記第3の暗号化回路に前記入力情報の初期値として入力する第2の抽出手段と、前記第3の暗号化回路による暗号化結果値を前記第2の鍵によって暗号化するとともに、この暗号化結果値を前記第3の暗号化回路に前記入力情報として更新入力する第4の暗号化回路と、前記パケットに格納されたデータと前記第4の暗号化回路の暗号化結果値との排他論理和を出力する第2の排他OR回路とを備えたことを特徴とする(請求項5に対応)。

## 【0014】

## 【作用】

(請求項1の作用) サービスプロバイダ内において鍵生成手段は、乱数に基づき2つの鍵を生成する。第1の暗号化手段は、この鍵生成手段により生成された2つの鍵に基づいて所定の暗号化アルゴリズムを実行することにより、データを暗号化する。また、第2の暗号化手段は、この2つの鍵を特定内容のマスタ鍵によって暗号化する。以上の後、データ配送手段は、第1の暗号化手段によって暗号化されたデータをサービスクライアントに配送し、鍵配送手段は、第2の暗号化手段によって暗号化された2つの鍵をサービスクライアントに配送する。

【0015】 一方、サービスクライアント内において、第1の復号化手段は、鍵配送手段によって配送された暗号化された2つの鍵を特定内容のマスタ鍵によって復号化する。第2の復号化手段は、この第1の復号化手段によって復号化された2つの鍵に基づいて、上記暗号化アルゴリズムに対応する復号化アルゴリズムを実行することにより、データ配送手段によって配送された暗号化されたデータを復号化する。

【0016】 このように、2つの鍵によって暗号化を行

っているので暗号化強度が強くなる。

（請求項 2 の作用）鍵生成手段は、乱数に基づき第 1 の鍵及び第 2 の鍵を生成する。第 1 の暗号化回路は、入力情報を第 1 の鍵によって暗号化する。この入力情報の初期値は、抽出手段によってパケットのヘッダから抽出された時刻情報である。初期値の暗号化を完了した後では、第 2 の暗号化回路の暗号化結果が入力情報となる。

【 0 0 1 7 】この第 2 の暗号化回路は、第 1 の暗号化回路による暗号化結果値を第 2 の鍵によって暗号化する。排他 OR 回路は、パケットに格納されたデータと第 2 の暗号化回路の暗号化結果値との排他論理和を出力する。

【 0 0 1 8 】このように、この暗号化処理方式では、暗号化のために第 1 の鍵、第 2 の鍵、及び時刻情報を用いている。そのため、暗号化強度がそれだけ向上する。しかも、時刻情報を用いているから、たとえ第 1 の鍵及び第 2 の鍵を暫く一定にしていたとしても、同じ内容のデータを別個の内容を持った暗号化データとすることができ、それだけ第三者による解読が困難になる。

（請求項 3 の作用）パケットがこのパケットに格納されているデータの格納位置についての格納位置情報を含むようにし、暗号化制御回路がこの格納位置情報に基づいてデータが排他 OR 回路に入力されている時点でのみ第 1 の暗号化回路及び第 2 の暗号化回路による暗号化を可能とするように制御を行えば、パケットのデータ格納部分以外を平文のままとしておくことができるので、サービスクライアントは、この平文部分から時刻情報を読み出して復号を行うことができる。

（請求項 4 の作用）パケットから時刻情報を検出して第 1 の暗号化回路及び第 2 の暗号化回路の状態を初期化する初期化手段を更に備えれば、サービスクライアント側に特別な同期信号を送信しなくても、サービスクライアントは、この時刻情報を検出して自律的に暗号同期をとることができる。

（請求項 5 の作用）サービスプロバイダにおいて鍵生成手段は、乱数に基づき第 1 の鍵及び第 2 の鍵を生成する。鍵配送手段は、この第 1 の鍵及び第 2 の鍵をサービスクライアントに配送する。また、第 1 の暗号化回路は、入力情報を第 1 の鍵によって暗号化する。この入力情報の初期値は、第 1 抽出手段によってパケットのヘッダから抽出された時刻情報である。初期値の暗号化が完了した後では、第 2 の暗号化回路による暗号化結果が入力情報となる。この第 2 の暗号化回路は、第 1 の暗号化回路による暗号化結果値を第 2 の鍵によって暗号化する。第 1 の排他 OR 回路は、パケットに格納されたデータと第 2 の暗号化回路の暗号化結果値との排他論理和を出力する。データ配送手段は、このようにして暗号化されたデータを格納したパケットをサービスクライアントに配送する。

【 0 0 1 9 】一方、サービスクライアントにおいて第 3 の暗号化回路は、入力情報を第 1 の鍵鍵配送手段によ

て配送された第 1 の鍵によって暗号化する。この入力情報の初期値は、第 2 の抽出手段によってパケットのヘッダから抽出された時刻情報である。この初期値の暗号化が完了した後は、第 4 の暗号化回路による暗号化結果が入力情報となる。この第 4 の暗号化回路は、第 3 の暗号化回路による暗号化結果値を第 2 の鍵によって暗号化する。第 2 の排他 OR 回路は、パケットに格納されたデータと第 4 の暗号化回路の暗号化結果値との排他論理和を出力する。

【 0 0 2 0 】このように、この暗号化処理方式では、暗号化のために第 1 の鍵、第 2 の鍵、及び時刻情報を用いている。そのため、暗号化強度がそれだけ向上する。しかも、時刻情報を用いているから、たとえ第 1 の鍵及び第 2 の鍵を暫く一定にしていたとしても、同じ内容のデータを別個の内容を持った暗号化データとすることができ、それだけ第三者による解読が困難になる。

【 0 0 2 1 】

【実施例】以下、図面に基づいて、本発明の一実施例の説明を行う。本実施例は、本発明による暗号化処理方式を、デジタル・オーディオ・インタラクティブ・システムに適用したものである。

《実施例の構成》

（ソフトウェアの構成）先ず、本実施例によるデジタル・オーディオ・インタラクティブ・システムにおいて流通されるソフトウェアの構成を、図 3 に示す。図 3 に示されるように、一本のソフトウェアは、複数に分割されて、夫々別のトランスポートパケット P に格納される。このトランスポートパケット P は、MPEG で規定されたものである。

【 0 0 2 2 】各トランスポートパケット P の先頭には、夫々のトランスポートパケット P に格納されているデータの状態を示すメインヘッダが付加されている。このメインヘッダには、データ識別 ID ( ID ) , 相対時刻情報 ( PCR ) , データ長情報 ( L ) , 等の各種情報が含まれている。即ち、データ識別 ID は、或るソフトウェアを構成するデータを格納していることを示す識別子であり、同じソフトウェアを構成するデータを格納している全てのトランスポートパケット P には同じデータ識別 ID が付されている。また、相対時刻情報 ( PCR ) は、各トランスポートパケット P の生成時刻を示す情報であり、次々と送られたデータの順番に従ってアップデートされてソフトウェア全体が送り終えた段階で停止するものである。従って、この相対時刻情報 ( PCR ) の順番に、データ識別 ID を同じくする各トランスポートパケット P に格納されているデータを並べることにより、元のソフトウェアを再構築することができる。また、格納位置情報としてのデータ長情報 ( L ) は、このメインヘッダの後に続くデータの長さを示す情報である。

【 0 0 2 3 】各トランスポートパケット P には、メイン

ヘッダに続いて、データとサブヘッダが交互に繋がっている。各データは、MPEG規格によって圧縮された1フレームの画像及び音声データである。また、各サブヘッダは、その後に続くデータの長さを示すデータ長情報(L)を含んでいる。

【0024】(システムの構成)次に、本実施例によるデジタル・オーディオ・インタラクティブ・システムの概略を、図2に示す。このデジタル・オーディオ・インタラクティブ・システムは、多数のソフトウェアを格納するとともにこのソフトウェアをクライアントからのリクエストに応じて配送するサービスプロバイダと、配送されたソフトウェアを受け取ってこれを再生する多数のサービスクライアントから、構成されている。本実施例によるデジタル・オーディオ・インタラクティブ・システムの構成は、データ識別ID(ID)及び時刻情報(PCR)を暗号化のために利用して、同一の平文データ(未暗号化のデータのことを言う。以下同じ。)が暗号化されても、常に、異なる内容の暗号文を作り上げる工夫をしたものである。以下、サービスプロバイダ及びサービスクライアント毎に、その詳細な構成を説明する。

【0025】〔サービスプロバイダ〕サービスプロバイダ内において乱数発生器1は、各ソフトウェアのタイトル毎に、1週間に一度、乱数系列を生成する。この乱数系列は、鍵ブロック単位(予め定められた暗号用鍵の桁)2個分の長さを有し、第1鍵バッファ16、第2鍵バッファ17、及び鍵用第1DES(Data Encryption Standard)4に入力される。

【0026】鍵生成手段としての第1鍵バッファ16は、この乱数系列から先頭の鍵ブロック単位を切り出して、これを第1タイトル鍵(Ks1)として、次の乱数系列の入力があるまでこの第1タイトル鍵(Ks1)を保持する。

【0027】同様に、鍵生成手段としての第2鍵バッファ17は、この乱数系列から2番目の鍵ブロック単位を切り出して、これを第2タイトル鍵(Ks2)として、次の乱数系列の入力があるまでこの第2タイトル鍵(Ks2)を保持する。

【0028】鍵用第1DES暗号化回路4は、第1タイトル鍵(Ks1)及び第2タイトル鍵(Ks2)からなる乱数系列を、第1マスタ鍵(K1)を用いて暗号化する。暗号化された乱数系列は、鍵用第2DES暗号化回路5に渡され、第2マスタ鍵(K2)を用いて更に暗号化される。

【0029】このようにして二重に暗号化された乱数系列は、特定のタイトルに対するタイトル鍵であるとして、鍵ファイル25内に一旦蓄えられる。この鍵ファイル25内に蓄えられた暗号化された乱数系列は、1週間後にそのタイトルに対する新たなタイトル鍵用の乱数系列が生成されると、これによって更新される。

【0030】一方、各タイトルのソフトウェアは、乱数発生器1から乱数系列が発生するのに合わせて、週に一回新たなタイトル鍵(Ks1、Ks2)によって暗号化されて、蓄積ファイル9に格納される。即ち、蓄積ファイル9に格納されている或るタイトルのソフトウェアは、週に一回更新されるのである。この更新を行うために、平文のデータを格納している同一識別ID(ID)を有するトランスポートパケットP群は、相対時刻情報(PCR)の順に処理を受ける。

【0031】個々のトランスポートパケットPのメインヘッダからは、識別ID(ID)及び相対時刻情報(PCR)が抽出されて、タイトル用第1DES暗号化回路6及びDESセット/リセット回路22に入力される(抽出手段に相当)。それと同時に、メインヘッダからデータ長情報(L)が抽出されて、データストロブ信号検出器21に入力される。なお、個々のトランスポートパケットPのサブヘッダからも、データ長情報(L)が抽出されて、データストロブ信号検出器(ST)21に入力される。このようにして各種情報が抽出されたトランスポートパケットPは、メインヘッダ側から順に排他OR回路8の一方の入力端子に入力される。

【0032】初期化手段としてのDESセット/リセット回路22は、入力されたデータから識別ID(ID)及び相対時刻情報(PCR)を検知すると、新たなトランスポートパケットPに対する処理が開始されたと判断して、タイトル用第1DES暗号化回路6及びタイトル用第2DES暗号化回路7をリセットしてそれらの内部状態を初期状態にする。この結果、本実施例では、各トランスポートパケットPの先頭において暗号同期がとられることになる。即ち、新たなトランスポートパケットPが入力されて識別ID(ID)及び相対時刻情報(PCR)が入力される毎に、両タイトル用DES暗号化回路6、7が初期化されて、この識別ID(ID)及び相対時刻情報(PCR)を初期値として暗号化が再開されることになる。

【0033】第1の暗号化回路としてのタイトル用第1DES暗号化回路6は、第1鍵バッファ16に保持されている第1タイトル鍵(Ks1)を用いて、入力情報を暗号化する。タイトル用第1DES暗号化回路6は、リセット後の初期状態においては、識別ID(ID)及び相対時刻情報(PCR)を初期値として暗号化するが、以後再度リセットされるまではタイトル用第2DES暗号化回路6から帰還されるデータを暗号化する。

【0034】第2の暗号化回路としてのタイトル用第2DES暗号化回路7は、第2鍵バッファ17に保持されている第2タイトル鍵(Ks2)を用いて、タイトル用第1DES暗号化回路6からの入力情報を更に暗号化する。この結果、攪乱性が更に高められる。タイトル用第2DES暗号化回路7の出力は、タイトル用第1DES暗号化回路6の入力端に帰還されるとともに排他OR回

路 8 の他方の入力端子に入力される。この帰還は、DES セット／リセット回路 2 2 によって各タイトル用 DES 暗号化回路 6, 7 がリセットされるまで繰り返される。

【0035】暗号化制御回路としてのデータストローブ信号検出器 (ST) 2 1 は、トランスポートパケット内のデータのみを暗号化処理するため、各トランスポートパケット P のメインヘッダからデータ長情報 (L) を抽出し、このデータ長情報 (L) に基づいて各タイトル用 DES 暗号化回路 6, 7 の暗号化を開始／停止させる制御信号、即ちデータストローブを出力する。即ち、このデータストローブは、各トランスポートパケット P 内における各データの頭部分が排他 OR 回路 8 に入力されたタイミングで、各タイトル用 DES 暗号化回路 6, 7 による暗号化を開始させ、各データの末端部分が排他 OR 回路 8 を通過したタイミングで、各タイトル用 DES 暗号化回路 6, 7 による暗号化を停止させるパルスである。なお、データストローブによって暗号化が停止されていると、タイトル用第 2 DES 暗号化回路 7 は、  
“0” を出力し続ける。

【0036】排他 OR 回路 8 は、平文のトランスポートパケット P の内容とタイトル用第 2 DES 暗号化回路 7 からの暗号化データとの排他論理和を出力する。即ち、排他 OR 回路 8 は、各トランスポートパケット P 内のヘッダ (メインヘッダ及びサブヘッダ) の部分が入力された時には、両タイトル用 DES 暗号化回路 6, 7 が暗号化を行っていないので、このヘッダの内容を平文のまま出力する。また、各トランスポートパケット P 内のデータの部分が入力された時には、両タイトル用 DES 暗号化回路 6, 7 が暗号化を行っているので、タイトル用第 2 DES 暗号化回路 7 からの暗号化情報に従って入力データの論理値を反転させて出力する。

【0037】このようにして、平文のヘッダ (メインヘッダ、サブヘッダ) を付した暗号化データが作り出され、蓄積ファイル 9 に蓄積される。同じ識別 ID を有する次の相対時刻情報 (PCR) を備えたトランスポートパケット P が処理対象になると、両タイトル用 DES 暗号化回路 6, 7 がリセットされて、そのトランスポートパケット P の識別 ID 及び相対時刻情報 (PCR) を初期値として新たな暗号化が行われる。このようにして、  
或るタイトルを構成する全ての暗号化データが蓄積ファイル 9 に蓄積されるのである。この時、同じタイトルのソフトウェアについての暗号化データが既に蓄積ファイル 9 内に蓄積されている時には、新たな暗号化データによって古い暗号化データを更新する。

【0038】このようにして蓄積ファイル 9 に蓄積された各タイトルの暗号化データ (トランスポートパケット P) は、何れかのサービスクライアントからの要求に応じて、相対時刻情報 (PCR) の順に蓄積ファイル 9 から読み出され、データ配送手段としてのトランスポート

層伝送路を介して要求元のサービスクライアントに配送される。このとき、配送される暗号化データ (トランスポートパケット P) のタイトルに対応する暗号化乱数系列も、鍵ファイル 2 5 から読み出され、トランスポート層のユーザ割当パケットの一部 (鍵配送手段としてのセッション層伝送路) を利用してサービスクライアントに配送される。

【0039】〔サービスクライアント〕サービスクライアント内において、セッション層伝送路を介して受信された暗号化乱数系列は、鍵用第 1 DES 復号化回路 1 2 に入力される。この鍵用第 1 DES 復号化回路 1 2 は、第 1 マスタ鍵 (K 1) 1 0 を利用して、鍵用第 1 DES 暗号化回路 4 と全く逆のアルゴリズムを実行して復号化を行う。なお、この第 1 マスタ鍵 (K 1) 1 0 は、サービスプロバイダ側のものと全く同じ内容の固定鍵である。

【0040】鍵用第 1 DES 復号化回路 1 2 の出力は、鍵用第 2 DES 復号化回路 1 3 に入力される。この鍵用第 2 DES 復号化回路 1 3 は、第 2 マスタ鍵 (K 2) 1 1 を利用して、鍵用第 2 DES 暗号化回路 5 と全く逆のアルゴリズムを実行して復号化を行う。なお、この第 2 マスタ鍵 (K 2) 1 1 は、サービスプロバイダ側のものと全く同じ内容の固定鍵である。

【0041】これら 2 段の復号化プロセスを通過した鍵用第 2 DES 復号化回路 1 3 の出力は、乱数発生器 1 から発生した乱数系列そのものとなる。この乱数系列は、第 1 鍵バッファ 1 8 及び第 2 バッファ 1 9 に夫々入力される。

【0042】第 1 鍵バッファ 1 8 は、この乱数系列から先頭の鍵ブロック単位を切り出して、これを第 1 タイトル鍵 (Ks 1) として、次の乱数系列の入力があるまでこの第 1 タイトル鍵 (Ks 1) を保持する。

【0043】同様に、第 2 鍵バッファ 1 9 は、この乱数系列から 2 番目の鍵ブロック単位を切り出して、これを第 2 タイトル鍵 (Ks 2) として、次の乱数系列の入力があるまでこの第 2 タイトル鍵 (Ks 2) を保持する。

【0044】一方、トランスポート層を介して受信されたトランスポートパケット P は、順番に排他 OR 回路 2 0 に入力される。この排他 OR 回路 2 0 に入力される前に、各トランスポートパケット P のメインヘッダからは、予め、識別 ID (ID) 及び相対時刻情報 (PCR) が抽出されて、タイトル用第 1 DES 復号化回路 1 4 及び DES セット／リセット回路 2 4 に入力される (第 2 の抽出手段に相当)。それと同時に、メインヘッダからデータ長情報 (L) が抽出されて、データストローブ信号検出器 2 3 に入力される。なお、個々のトランスポートパケット P のサブヘッダからも、データ長情報 (L) が抽出されて、データストローブ信号検出器 (ST) 2 3 に入力される。

【0045】DESセット／リセット回路24は、入力されたデータから識別ID（ID）及び相対時刻情報（PCR）を検知すると、新たなトランスポートパケットに対する処理が開始されたと判断して、タイトル用第1DES暗号化回路14及びタイトル用第2DES暗号化回路15をリセットしてそれらの内部状態を初期状態にする。なお、上述したように、本実施例では、各トランスポートパケットの先頭において暗号同期がとられる。従って、通信路の誤り及び切断があった時には、サービスクライアント内において、次のトランスポートパケットの先頭を検出して両タイトル用DES暗号化回路14、15をリセットすれば、自律的に同期状態に復帰することができる。

【0046】第3の暗号化回路としてのタイトル用第1DES暗号化回路14は、第1鍵バッファ18に保持されている第1タイトル鍵（Ks1）を用いて、入力データを、サービスプロバイダのタイトル用第1DES暗号化回路6と同じアルゴリズムで暗号化する。タイトル用第1DES暗号化回路14は、リセット後の初期状態においては、識別ID（ID）及び相対時刻情報（PCR）を初期値として暗号化するが、以後再度リセットされるまではタイトル用第2DES暗号化回路15から帰還されるデータを暗号化する。

【0047】第4の暗号化回路としてのタイトル用第2DES暗号化回路15は、第2鍵バッファ19に保持されている第2タイトル鍵（Ks2）を用いて、タイトル用第1DES暗号化回路14からの入力データを、サービスプロバイダのタイトル用第2DES暗号化回路7と同じアルゴリズムで更に暗号化する。タイトル用第2DES暗号化回路15の出力は、タイトル用第1DES暗号化回路14の入力端に帰還されるとともに排他OR回路20の他方の入力端子に入力される。この帰還は、DESセット／リセット回路24によって各タイトル用DES暗号化回路14、15がリセットされるまで繰り返される。

【0048】データストローブ信号検出器（ST）23は、トランスポートパケットP内のデータのみを暗号化処理するため、各トランスポートパケットPのメインヘッダからデータ長情報（L）を抽出し、このデータ長情報（L）に基づいて各タイトル用DES暗号化回路14、15の暗号化を開始／停止させる制御信号、即ちデータストローブを出力する。即ち、このデータストローブは、各トランスポートパケットP内における暗号化されたデータ部分が排他OR回路20に入力されている時のみ、各タイトル用DES暗号化回路14、15による暗号化を行わしめるパルスである。なお、データストローブによって暗号化が停止されていると、タイトル用第2DES暗号化回路15は、“0”を出力し続ける。

【0049】以上のように、サービスクライアントにおける第1鍵バッファ18及び第2鍵バッファ19以降の

回路は、サービスプロバイダのものと全く同じである。従って、排他OR回路20に入力されるタイトル用第2DES暗号化回路15からの暗号化情報も、サービスプロバイダにおける排他OR回路8に入力されるタイトル用第2DES暗号化回路7からの暗号化情報と全く同じである。そのため、排他OR回路20は、各トランスポートパケットP内のヘッダ（メインヘッダ及びサブヘッダ）の部分が入力された時には、このヘッダの内容を平文のまま出力する。また、各トランスポートパケットP内のデータの部分が入力された時には、タイトル用第2DES暗号化回路15からの暗号化情報に従って論理値を反転させて出力する。この暗号化データは、暗号化によってその論理値が元々反転されていたものである。よって、排他OR回路20における再反転によって、その論理値が元の状態に戻るのので、暗号化前の平文のデータを復元することができるのである。

《実施例の作用》以上のように、本実施例では、サービスプロバイダ及びサービスクライアント側双方において、タイトル用DES暗号化回路を二重にしている。従って、暗号化アルゴリズムが強化されているので、第三者（ユーザを含む）がトランスポートパケットに基づいて二つのタイトル鍵を解読して、暗号化データを復号化することが、非常に困難となった。このことを図4及び図5を基づいて説明する。

【0050】いま、かりに、タイトル用第1DES暗号化回路14に値“1”を入力したら、タイトル用第2DES暗号化回路15の出力端に値“0”が出力されたとする。この場合に第1鍵バッファ18及び第2鍵バッファ19に保持されているタイトル鍵Ks1、Ks2を解読するには、図4に示すように、タイトル用第1DES暗号化回路14に既知の値“1”を入力し続け、本来のタイトル鍵Ks1に変えて種々の値（推定鍵：Ks1m）とこれらに対するタイトル用第1DES暗号化回路14の出力値“C”を測定する。そして、測定された推定鍵（Ks1m）と出力値“C”との関係を、図5に示すように表30にまとめる。

【0051】同様に、タイトル用第2DES暗号化回路15に種々の推定鍵（Ks2m）を入力して、このタイトル用第2DES暗号化回路15の出力が既知の値“0”を維持する入力値“C”を測定する。そして、測定された推定鍵（Ks2m）と入力値“C”との関係を、図5に示すように表32にまとめる。

【0052】このようにして作成した二つの表30、32を対比した場合に、両表に同じ中間値“C1k”が表れたら、この値“C1k”に対応する推定鍵“Ks1”，“Ks2”が、夫々第1タイトル鍵Ks1、第2タイトル鍵Ks2であると解読できる。

【0053】このような鍵の解読法（鍵総暗探解読：中間一致攻撃）は、しかしながら、多くの処理時間とメモリ資源を必要とする。例えば、70ビットの平文、暗号



文ペアの場合には、 $2^{56}$  回の手続き回数が必要であり、また、上記表を作成するために  $2^{56}$  ワード（1 ワード 64 ビット）のメモリが必要になる。従って、内部 16 段の DES 回路を 2 段にすると、事実上解読が困難になるのである。

【0054】なお、比較のために、DES 回路を一段にしたときの鍵総暗探解読を説明すると、既知の入力値に対して既知の出力値を出力する推定鍵を探し出すだけで良いので、処理の手間が大幅に経る。上記例に沿うと、70 ビットの平文、暗号文ペアの場合には、 $2^{56}$  回の手続 10 手続き回数のみで成功可能であるので、Wiener の 10 万ドル装置で 35 時間程度で解読できてしまう。その結果、本実施例では、タイトル鍵の更新を週 1 回程度にすることができる。よって、通信路容量をタイトル鍵配送のために消費してしまう問題を解決し、サービスプロバイダ—サービスクライアント間の情報転送効率を向上させることができる。

【0055】なお、このようなタイトル鍵配送回数を激減させるには、暗号同期を鍵更新から切り離して行う必要が、副次的に生じる。本実施例では、暗号同期を、デ 20 ータを配送するためのトランスポートパケットのヘッダに格納されている識別 ID (ID) と相対時刻情報 (PCR) によって行っているので、タイトル鍵配送回数を激減させても暗号同期を行うことができる。しかも、この相対時刻情報 (PCR) がトランスポートパケットの生成時間に依って異なる値をとる。従って、全く同じ内容の平文データが暗号化される場合でも、この平文データを暗号化したデータは全く異なるデータとなる。

【0056】

【発明の効果】以上のように構成された本発明の暗号化 30 処理方式によると、鍵の頻繁な変更が少なくなり、また、暗号同期信号はシステムに予め備わっている時刻情

報を活用することから、暗号アルゴリズムの強化及び暗号同期の為、ユーザパケットの一部を犠牲にする必要がなくなる。

【図面の簡単な説明】

【図 1】 本発明の原理を示す原理図

【図 2】 本発明の一実施例による暗号化処理方式が適用されたデジタル・オーディオ・インタラクティブ・システムの概略図

【図 3】 一つのソフトウェアを構成するデータが格納された各トランスポートパケットの構造を示す説明図

【図 4】 中間一致攻撃による鍵総暗探解読方式の説明図

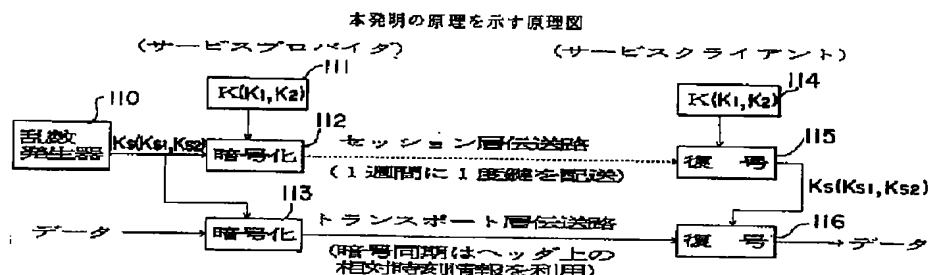
【図 5】 中間一致攻撃による鍵総暗探解読方式の説明図

【図 6】 従来の暗号化処理方式の概略説明図

【符号の説明】

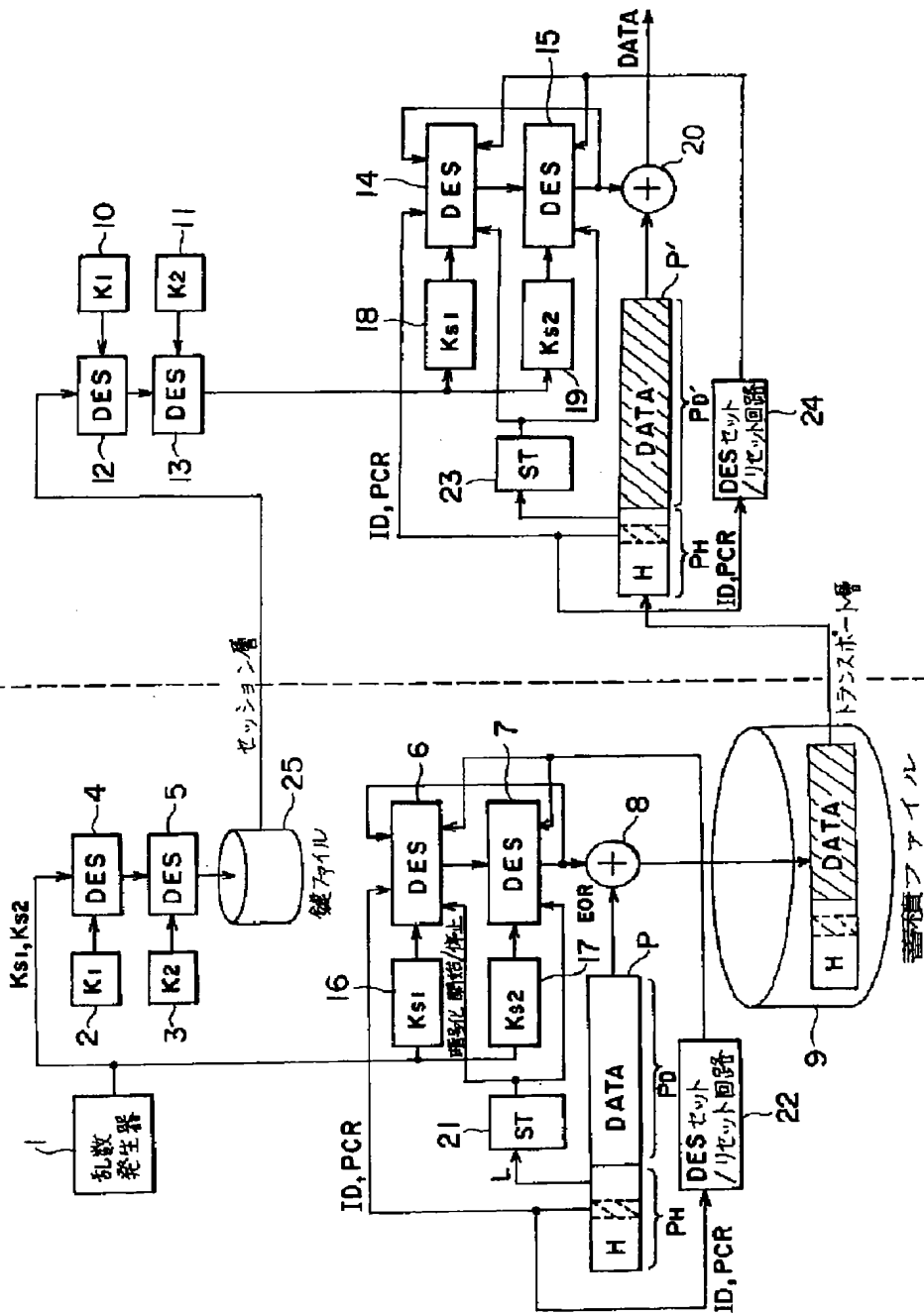
- 1 乱数発生器
- 6 タイトル用第 1 DES 暗号化回路
- 7 タイトル用第 2 DES 暗号化回路
- 8 排他 OR 回路
- 14 タイトル用第 1 DES 暗号化回路
- 15 タイトル用第 2 DES 暗号化回路
- 16 第 1 タイトル鍵バッファ
- 17 第 2 タイトル鍵バッファ
- 18 第 1 タイトル鍵バッファ
- 19 第 2 タイトル鍵バッファ
- 20 排他 OR 回路
- 21 データストローブ信号検出器 (ST)
- 22 DES セット/リセット回路
- 23 データストローブ信号検出器 (ST)
- 24 DES セット/リセット回路

【図 1】



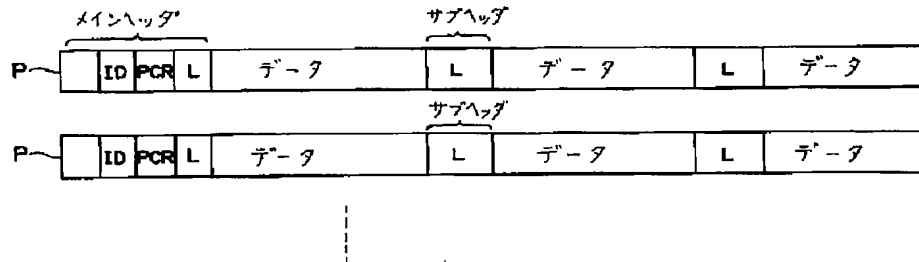
【 図 2 】

本発明の一実施例による暗号化処理方式が適用されたデジタル・オーディオ・インタラクティブ・システムの概略図  
 サービスマスタ側  
 [クライアント側]



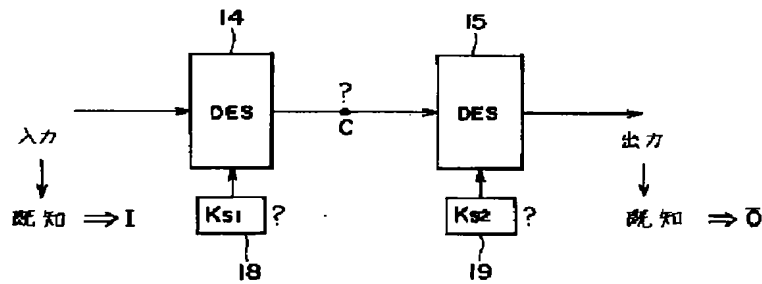
【図 3】

一つのソフトウェアを構成するデータが格納された各トランスポートパケットの構造を示す説明図



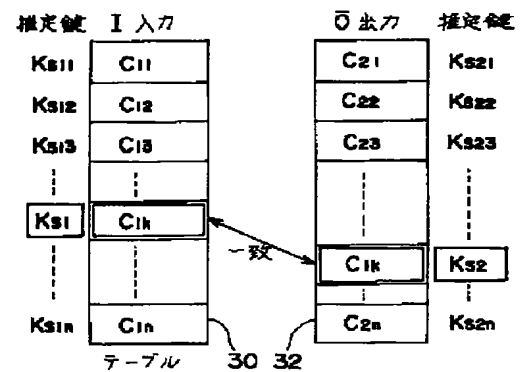
【図 4】

中間一致攻撃による鍵総暗探解読方式の説明図



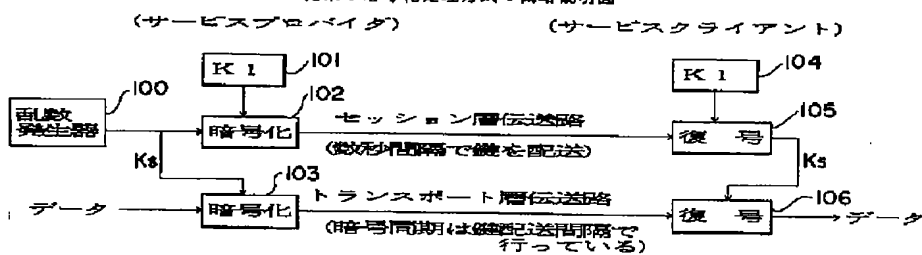
【図 5】

中間一致攻撃による鍵総暗探解読方式の説明図



【図 6】

従来の暗号化処理方式の概略説明図



フロントページの続き

(51) Int. Cl.

識別記号

庁内整理番号

F I

技術表示箇所

9/12

H04N 7/167

- (72) 発明者 古賀 譲  
神奈川県川崎市中原区上小田中 1 0 1 5 番  
地 富士通株式会社内
- (72) 発明者 石崎 正之  
神奈川県川崎市中原区上小田中 1 0 1 5 番  
地 富士通株式会社内
- (72) 発明者 吉岡 誠  
神奈川県川崎市中原区上小田中 1 0 1 5 番  
地 富士通株式会社内